CLAIMS

What is claimed is:

Sub B2

1. A method for electronic commerce, comprising:

sending from a merchant's computer over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

sending from said consumer's computer consumer identity and authentication information and said merchant message, to an issuer gateway for an issuing bank;

verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

2. The method for electronic commerce of claim 1, which further comprises:

27

sending from said consumer's computer a start message over the internet network to the merchant's computer, to initiate said merchant's message.

3. The method for electronic commerce of claim 1, wherein said wallet initiation message includes a nonce.

4. The method for electronic commerce of claim 1, wherein said merchant's computer further performs the steps comprising:

receiving said authorization token;

verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token;

verifying the freshness of the authorization token via the timestamp in the token;

using the nonce in the authorization token to recognize duplicate tokens; and

fulfilling said order description.

5. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a userid and a password.

6. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is an ATM debit card number and PIN.

7. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a smart card's account number and a symmetric Message Authentication Code (MAC).

8. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a smart card's account number and an asymmetric digital signature.

9. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a consumer's digital signature and digital certificate.

11

10. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a consumer's digital certificate and matching asymmetric digital signature.

12

11. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a is a user account number and a symmetric MAC or asymmetric digital signature.

13

12. The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a is a user account number and an asymmetric digital signature.

14

13. The method for electronic commerce of claim 1, wherein said consumer identity information is a consumer's biometric signal.

15

14. The method for electronic commerce of claim 1, wherein said issuer gateway sends said authorization token to said consumer, and the consumer forwards said authorization token to said merchant.

16

15. The method for electronic commerce of claim 1, wherein said issuer gateway sends said authorization token directly to said merchant.

94

17 16. The method for electronic commerce of claim 1, wherein said reference to said credit card is an alias card number that is mapped at the issuing bank to the real card number, thereby preventing use of the consumer's credit card number without said authorization token.

18 17. The method for electronic commerce of claim 1, wherein said reference to said card is an authorization number allocated uniquely by the issuer gateway for each authorization, enabling it to be passed by an acquirer gateway back to the issuing bank in a capture message;

said issuing bank maintaining a database mapping authorization numbers to card numbers, so that when the issuing bank receives the capture message, it uses the database mapping to determine the consumer's card number.

Sub A6 7 ~~18. The method for electronic commerce of claim 9, wherein said authorization token~~ includes a ~~dummy~~ card number for use in routing payment to an appropriate one of a plurality of issuing banks;

~~said dummy card number being shared among all cardholders of a particular issuing bank.~~

19. The method for electronic commerce of claim 1, which further comprises:

a digital certificate hierarchy that covers issuing banks, acquiring banks, and merchants.

20. The method for electronic commerce of claim 19, wherein said certificate hierarchy is used with public-key digital signatures to identify said merchant and said issuing bank.

21. The method for electronic commerce of claim 20, wherein said certificates represent common financial agreements and obligations among said merchant and said issuing bank.

22. The method for electronic commerce of claim 21, wherein the issuing bank certificates identify and help authenticate issuing banks to merchants, providing a basis for the merchants to trust the authorization tokens provided by the issuing banks.

23. The method for electronic commerce of claim 22, wherein an acquiring bank certificate and a merchant certificate identify and help authenticate said acquiring bank and said merchant to issuing banks;

said merchant certificate identifying the merchant to the consumer and verifying that the merchant is a valid participant of a payment scheme, before the issuing bank provides said authorization token.

24. The method for electronic commerce of claim 1, wherein split shipments are supported by an additional message interaction between the merchant and issuer gateway, comprising:

the merchant sending the authorization token to the issuer gateway identified in the issuer's digital certificate, including details of a split requirement, such as the amount of a first payment, the merchant authenticating the request by signing it and including the merchant's digital certificate;

the issuer gateway verifying that the merchant signing message is the same merchant that signed an original request , verifying the split request according to business and risk management policies, and responding with a new authorization token in a message to the merchant;

the merchant forwarding the new authorization token in a capture message the acquirer gateway;

the merchant resubmitting the new authorization token to the acquirer gateway in a second message, whenever the merchant has shipped a second part of the shipment.

25. The method for electronic commerce of claim 1, Japanese Payment Options are provided, comprising:

31

the issuer offering special payment arrangements to the consumer, conditioned on the merchant name from the merchant's digital certificate and the amount of payment from the initiation message.

26. A system for electronic commerce, comprising:

a merchant's computer for sending over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

a consumer's wallet program in said consumer's computer responsive to said wallet initiation message, for sending from said consumer's computer consumer identity and authentication information and said merchant message, to an issuer gateway for an issuing bank;

an issuer gateway for verifying said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

27. A computer program product, comprising:

computer program code means for sending from a merchant's computer over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

computer program code means for starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

computer program code means for sending from said consumer's computer consumer identity and authentication information and said merchant message, to an issuer gateway for an issuing bank;

computer program code means for verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

28. A data processing system for electronic commerce, comprising:

a computer processor means for sending from a merchant's computer over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank,

said wallet initiation message including a payment amount, an order description, and a timestamp;

means for starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

means for sending from said consumer's computer consumer identity and authentication information and said merchant message, to an issuer gateway for an issuing bank;

means for verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

33 32

~~29~~. The data processing system for electronic commerce of claim ~~28~~, which further comprises:

means for sending from said consumer's computer a start message over the internet network to the merchant's computer, to initiate said merchant's message.

34 32

~~30~~. The data processing system for electronic commerce of claim ~~28~~, wherein said wallet initiation message includes a nonce.

35 32

31. The data processing system for electronic commerce of claim 28, wherein said merchant's computer further comprises:

means for receiving said authorization token;

means for verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token;

means for verifying the freshness of the authorization token via the timestamp in the token;

means for using the nonce in the authorization token to recognize duplicate tokens; and

means for fulfilling said order description.

36 32

32. The data processing system for electronic commerce of claim 28, wherein said reference to said credit card is a consumer credit or debit account number.

33. A method for electronic commerce, comprising:

sending from a merchant's computer over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

said acquiring bank's digital certificate containing a network address or URL that identifies the network location of said acquiring bank contacted via an internet network as part of a payment protocol;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

33

sending from said consumer's computer consumer identity and authentication information and said merchant message, to an issuer gateway for an issuing bank;

verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said issuer's digital certificate containing a network address or URL that identifies the network location of the issuer contacted via an internet network as part of a payment protocol;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

34. A method for electronic commerce, comprising:

sending from a consumer's computer consumer to an issuer gateway for an issuing bank, an authorization request message containing consumer identity and authentication information, payment amount, an order description, a timestamp, a digital certificate representing a merchant, and a digital certificate representing the merchant's acquiring bank;

said merchant's digital certificate containing a merchant identifier unique for the acquiring bank;

said acquiring bank's digital certificate containing a bank identifier unique among all banks sharing a common financial arrangement;

validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant, acquirer, and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce, said merchant identifier from the merchant's digital certificate, and said acquiring bank identifier from said acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number;

said authorization token being digitally signed by the issuing bank; and

said merchant's computer receiving said authorization token and fulfilling said order description.

39 38

35. The method for electronic commerce of claim 34, which further comprises:

sending from a merchant's computer over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital certificate, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

said consumer's wallet program sending the authorization request message.

40 39

36. The method for electronic commerce of claim 35, which further comprises:

34

including with the wallet initiation message a merchant's digital signature of the wallet initiation message;

including the wallet initiation message and said merchant's digital signature in the authorization request message;

verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant.

41 40
37. The method for electronic commerce of claim 36, which further comprises:

sending from said consumer's computer a start message over the internet network to the merchant's computer, to initiate said merchant's message.

42 40
38. The method for electronic commerce of claim 36, wherein said wallet initiation message includes a nonce.

43 40
39. The method for electronic commerce of claim 36, wherein said merchant's computer further performs the steps comprising:

receiving said authorization token;

verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token;

verifying the freshness of the authorization token via the timestamp in the token;

using the nonce in the authorization token to recognize duplicate tokens; and

fulfilling said order description.

36

44 38
40. The method for electronic commerce of claim 34, wherein the merchant claims payment through the acquiring bank by forwarding the customer reference number and payment amount to the acquiring bank.

45 44
41. The method for electronic commerce of claim 40, where in the case of a subsequent dispute, the merchant proves payment authorization by submitting a copy of the authorization token and issuer's digital certificate to the acquiring bank.

46 38
42. The method for electronic commerce of claim 34, wherein the merchant claims payment through the acquiring bank by forwarding the authorization token and issuer's digital certificate to the acquiring bank;

the acquiring bank verifying the issuer's signature on the authorization token, validating the issuer's digital certificate, checking for duplicates via the timestamp in the authorization token; and the acquiring bank paying the amount indicated in the authorization token.

47 38
43. The method for electronic commerce of claim 34, wherein said authorization request message and authorization token includes a hash of an order description instead of the actual order description, the order description itself being available separately at the merchant, the merchant validating that the authorization token refers to the same order description by comparing the hash of the order description in the authorization token against a locally-computed hash of the same order description.

48 38
44. The method for electronic commerce of claim 34, wherein said reference to said credit card is a consumer credit or debit account number.

49 48
45. The method for electronic commerce of claim 44, wherein the confidentiality of said credit or debit account number is maintained by using a higher-level security protocol, such as encrypted email or SSL, to protect the communications among the consumer and the issuer gateway, the consumer and the merchant, the issuer gateway and the merchant, and, if applicable, the merchant and the acquirer.

ADD B5 add C4

36